EAC Certification Program – Phase 2
Reducing Cost, Improving Effectiveness

By

Stephen Berger
stephen.berger@ieee.org
Technical Reviewer, US Election Assistance Commission

A Paper Prepared for the EAC Cost of Testing Workshop January 29-30, 2009 Miami, FL

Abstract

This white paper has been prepared as a contribution to the EAC "Cost of Testing Workshop" scheduled to be held January 29-30, 2009 in Miami, FL. Approximately two years into the EAC's voting system certification program there is a concern by many that certification is taking too long, costing too much and is not as effective as it could be. In response the EAC has scheduled this cost of testing workshop. The workshop is intended to bring all stakeholders together to examine the current state of the program and explore ways it might be reformed.

This white paper is prepared as a contribution to that effort. It is written from the perspective of a technical reviewer for the EAC. Important insights and input has been contributed through consultation with other stakeholders to the process. In the end the deficiencies of the paper undoubtedly arise from the limitations of the author. It merits will tend to arise from the insights obtained through collegial collaboration.

The analysis proposed is that the current certification program could benefit from both structural and technical reforms. In some cases technical reforms will require structural changes. Some suggestions are offered in each area.

Outline

Introduction

This paper is divided into two large sections:

- Technical reforms
- Structural reforms

In some cases the suggested changes are independent and can separately from other suggestions. In other cases changes are linked and must be made together. In the discussion the linkage or independence of various suggestions will be made clear.

General observations are that the certification process is currently:

- labor intensive
- requirements are often technically ambiguous or insufficiently specified to allow objective assessment
- there are too many requirements, often proscribing symptoms rather than dealing with underlying architectural issues
- there is no standardization between vendor systems, requiring that each evaluation be highly customized to each system submitted
- the certification process is too heavily loaded on the certification testing at the expense of design review and analysis, which could be performed much earlier and field surveillance, which would insure any missed problems are addressed
- certification is divorced from election administration, requiring that the system be fully compliant under any conceivable management process.

Based on these observations, suggestions for improvement are:

- Introduce automation, particularly in areas that currently require a lot of time
- Further specify requirements, perhaps through standardized test methods so that they are technically specific and unambiguous
- Group related requirements and were underlying issues can be identified, require sound architecture as opposed to only addressing symptoms
- Develop an industry wide model, especially for key interfaces. An example would be standardizing ballot definition and cast vote record formats so that the same inputs could be used for all systems.
- Introduce much more system analysis rather than rely totally on highly manual testing
- Allow systems to be certified with clearly stated assumptions about election management processes that are particularly important for a particular system.

These general themes are further described in the rest of this paper.

Technical Reforms

A variety of technical reforms are possible. Certain themes for improvement offer guidance on the areas that offer promise for improvement. Among those themes are:

- Use automation to make certification a less labor intensive process. Automation should reduce expense, speed up testing and improve its quality.
- Design systems to be testable & auditable.

Automating Source Code Review

Estimates are that source code review is currently taking about 45% of the cost of certification. It is therefore a priority target for improvement.

To analyze the current source code review process and look for potential improvements the question must first be ask, what is source code review intended to accomplish? In answer the following might be suggested:

- Source code review increases the public's confidence that malicious code has not been inserted into voting system software.
- It improves vendor quality by requiring commenting and coding conventions be followed.
- It provides information to guide the physical testing of the system. In this role examination of the code reveals different options that should be exercised during physical testing.
- It provide insight into the interface and relationship between software modules.
- It provides insight into the use of external resources in the operating system and other COTS software.
- It provides for review of sections of the code unreached by physical testing.

As currently practices most of the effort of source code review seems to go to the first two objectives, giving the public assurance that someone independent of the vendor has examined the software. Given the estimated cost the current method of source code review does not appear to deliver sufficient value.

Hybrid System Testing

System testing using mock primary and general elections is currently a highly manual process, requiring great effort to case a relatively small number of ballots and testing systems with typically 4-6 mock elections. However, taking a hybrid approach offers the opportunity to do much more testing while simultaneously reducing costs.

A voting system can be analyzed as voting stations (DRE's and Optical Scanners) and accumulation/tabulation software. With voting stations we want to know that they will accurately record the cast vote records for a wide variety of ballot styles, a wide variety of voting patterns and large number of voters. Testing of voting stations is amenable to automation.

The accumulation/tabulation software may be required to process a wide variety of ballot styles, a wide variety of input combinations (number of memory modules, number of votes on each modules, etc.) and a wide variety of input timings.

Design for Testability

Design for testability is a common industry practice. Many product development organizations have discovered that bringing in the test personnel at the end of the product development cycle is inefficient. If a product is not easily tested it can cause significant program delays and add unnecessary cost. A solution is to have the test personnel involved from the system concept stage.

An implementation in the certification process would be to engage VSTL engineers and EAC technical reviewers at the product specification stage. The question to be asked at that point would be, how would you test the system being conceived? At that point it is relatively easy to ask for test points, test interfaces and other facilities that would substantially improve testability of the system. Early engagement also allows time for the parallel development of test fixtures and automation.

An example of the value of early engagement for design for testability can be seen considering the hybrid test approach discussed above.

Structural Reforms

System Analysis

Many issues do not require testing to uncover. A design review, analyzing the system can reveal vulnerabilities and potential risks before any testing is performed and even before systems are designed. Early identification of problems or risks is both efficient and often more effective that testing. Analysis does not replace testing, but supplements it, often avoiding substantial time and expense. Particularly where a system is a revision of a currently deployed system part of a system analysis is to review the field experience of the previous version. A great deal can be learned and brought forward early, allowing vendors to address issues identified in their development plans.

The improvement recommended then would be to make available, at a vendor's option an early design review. If a vendor wishes to have a system pre-reviewed for compliance this option would make available to them insight as to the potential compliance problems with their system.

Assumed Administrative Procedures

Currently there is no means by which a voting system can be certified with a clear statement about the assumptions as to how it will be used. VSTL's and the EAC do not have the ability to say, "This system is being certified under that understanding that all users of the system will do the following…". The lack of ability to do this allows mistakes to be made in two directions, making requirements too hard in some areas and missing issues in others.

Certification takes place in isolation from election administration. At times assumptions are made about how voting systems will be used. These assumptions are made typically

by VSTL personnel who have relatively little direct experience with election administration and certainly do not have a broad sampling of the breadth and diversity of election administration. It is not uncommon for a vendor submitting a system to tutor its VSTL in the way their system is 'always' used. It is very possible for mistaken assumptions to be made, leading to significant mistakes.

On the one hand if the VSTL assumes a system will be always used in a certain way that that assumption is not true, the system will not be tested in the way it is sometimes, perhaps often used. This can lead to vulnerabilities of the system being missed. Since the VSTL does not document in the certification documentation their assumptions they are never reviewed and therefore prone to go uncorrected. Having the ability to state those assumptions in the certification test plan and later test report would make them amenable to review and, if needed, correction.

The lack of ability to state assumptions about how the system will be used commonly leads to requirements being applied more harshly than may be necessary. It is not uncommon that a system, in isolation, has a vulnerability, but a very reasonable and common administrative procedure would adequately protect against its manifestation. As example might be a system that is certified with the statement, "This system is being certified with the assumption that the pre-election L&A testing will always include the following features…". In this way, should a system be capable of being incorrectly configured for an election, that possibility would be mitigated. Currently the VSTL's only choice is to fail the system.

Mandated Development Plan

An extension of the lack of ability to clarify assumptions about election administrative practices is the lack of a facility for a mandatory development plan. Currently a certification decision must be made solely based on an assessment of a system passing or failing the VVSG. Underlying this condition is the assumption that there are no degrees of compliance or grey areas.

In contrast to the relatively wooden approach, 'it passes or fails', is the fact that often an established vendor will bring an improved version of a system. Previous versions of the system are in use and have an established field experience that may be examined. The revised system may well be an improvement over what is currently in use. However, on examination areas of further improvement, perhaps very important areas, may be identified. Currently the only available choice is to reject the improved system because of its need for further improvement. This denies election officials the use of the improved system and denies the company the revenue they may need for further development. In some cases, a preferable alternative would be to certify the improved system with a mandatory development plan to address identified deficiencies. In many cases such improvements could be introduced as field upgrades to any systems deployed.

A common scenario is one in which security concerns call for a defense-in-depth, with multiple levels of security at key points. A system may not have as many layers of protection as may be desirable. However, it does have protections, perhaps provided through good election administration. In such cases a responsible decision may be to

certify the system with a negotiated development plan with the vendor to reinforce the points of concern in the system.

It must be recognized that providing administrative capabilities like clarifying assumptions about election administration practices with a system and the ability to mandate a development plan in no way means that such tools are always appropriate. For many issues a system must be denied certification until issues are adequately remedied. However, there are other circumstances where the availability of such tools would be both appropriate and helpful.

Declaration of Conformity

Supplier Declaration of Conformity (DoC) is a regulatory method used by many agencies where the circumstances warrant it. The FCC uses DoC to regulate unintentional radiators, of which voting systems are an example. The European Commission uses DoC for most products under its CE mark program. Under a DoC program the vendor makes a legally binding representation that their product meets a set of specification. The regulator accepts that representation until there is reason to check it. The regulator may perform market audits to confirm that vendors are accurate in their representation. They may ask for documented evidence to support a claim and may, particularly where there is evidence that raises doubt, require testing of a product.

DoC would seem to be an option for some VVSG requirements. An example would be the radiated and conducted emissions requirements. These requirements are required by the FCC and by the VVSG. The FCC uses the DoC method to administer these requirements for unintentional radiators like voting equipment. They also have a very active and effective enforcement branch that works to assure that vendor representations are accurate. So in this case, with another federal agency requiring the same thing accepting a DoC and eliminate would seem to be a possibility.

Another possibility would be temperature and humidity testing. Allowing DoC for temperature and humidity requirements would seem to be a relatively low risk. If a systems design or field experience suggest there might be a problem then evidence to support the vendors claim could be required or testing performed.

Allowing some requirements to be covered by a supplier DoC would same time and cost in the certification process. It would also allow the certification process to focus on its core mission and requirements for which DoC is not appropriate.

Conclusions

This paper was prompted by the belief that significant cost reductions are possible for the voting system certification program. It appears that some of those savings are possible with improved efficiency. To obtain these savings and improvement will require implementing both technical and structural innovations.

Technically the key themes are to reduce labor cost by automating tests that are amenable to automation. Two examples are given, automated source code review and automated component testing.

Structurally recommendations include grouping requirements, to decrease the number of testable requirement, focusing testing on core requirements and providing administrative tools to allow certification to be connected to election administration practices.